USDA UNITED STATES DEPARTMENT OF AGRICULTURE

Information Systems Security Assessment Guide

Version 1.0

April 12, 2001

OCIO Cyber Security Program Office

U.S. Department of Agriculture

Washington, D.C. 20250

USDA Information Systems Security Assessment Guide

Purpose

This Security Assessment Guide is designed to assist Agency ISSPMs in satisfying their responsibility to develop and implement a comprehensive risk management program as defined in DR 3140-001, "USDA Information Systems Security Policy." By using this guide, Agency ISSPMs can identify areas where Department Information Security requirements are not being met and develop an action plan to ensure all security requirements are satisfied.

Scope

This guide is to be used by all USDA organizational elements to help assess the security posture of the element, ADP facilities within the element, and AIS that support the element.

Background

Risk Assessments are mandated by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." A security risk assessment process is a comprehensive evaluation of the system's technical and non-technical security features. It establishes the extent that a specific design and implementation meets specific security requirements. USDA does not currently have a comprehensive security risk assessment process. This guide is intended to serve as an interim measure, until formal risk assessment policies and procedures can be developed and implemented.

References

a. External

(1) Public Law 100-235, "Computer Security Act of 1987"
(2) Public Law 93-579, "Privacy Act of 1974"
(3) Public Law 93-502, "Freedom of Information Act"
(4) Public Law 99-474, "Computer Fraud and Abuse Act"
(5) OMB Circular No. A-130 Appendix III, "Security of Federal Automated Information Resources," revised February 8, 1996.
(6) OMB Circular No. A-123, "Management Accountability and Control," June 29, 1995.

b. USDA Internal Regulations

(1) DR 3140-001, "USDA Information Systems Security Policy" dated may 15, 1996

Abbreviations

AIS	Automated Information Systems
ADP	Automated Data Processing
ART	Acquisition Review Team

DISSPM	Departmental Information System Security Program Manager
DOS	Disk Operating System
FOISM	Field Office Information Security Managers
GAO	General Accounting Office
IRM	Information Resources Management
ISPO	Information Service Processing Organization
IS	Information System
ISSPM	Information Systems Security Program Manager
ISSP	Information System Security Program
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PACC-IRM	Policy Analysis and Coordination Center-Information Resources Management
SIRMO	Senior IRM Official
TCP/IP	Transmission Control Protocol/Internet Protocol
WAN	Wide Area Network
WP	Word Processing
USDA	United States Department of Agriculture

Assessment Process

The assessment process by its nature is hierarchical. There are requirements that must be satisfied at the Department, agency, or organizational element level. Other requirements are the responsibility of managers of ADP facilities that may host several systems or applications. Finally, each AIS system owner must take whatever steps are necessary to ensure that its sensitive IT resources are adequately protected.

This guide is structured to support a hierarchical approach. The following sections contain assessment guides to be completed at the agency level, the facility level, and at the AIS level. It is incumbent on the AIS system owner to ensure that agency and facility assessments have been completed and that potential risks resulting from requirements that have not been met at these levels are addressed.

Agency Assessment Guide

This assessment should be completed by the Agency's ISSPM or designated alternate. Answer all questions. Provide supplemental information as appropriate. All "No" answers must include supplemental information and an action plan that describes how the requirement will be met, as well as a schedule for completion of the plan. Typically, this would be done by developing the action plan in this document and reflecting this in the security plan for the agency.

Agency Identification:

Agency

(Agency, Office,
Bureau, Service, etc.):

Address

CIO Phone:

ISSPM Phone:

Date of last
Assessment:

The USDA is required to have an Information Systems Security Program (ISSP) that ensures adequate security of all USDA information, all AISs, and their supporting telecommunications. The foundation of this is the designation of an agency ISSPM who is responsible for executing an effective ISSP for the agency. The following questions will assist you in addressing this requirement.		YES	NO	PARTIAL
1	Has the agency designated, in writing, an ISSPM with appropriate authority and responsibility to manage the sensitive AIS and network security program? If no, provide the steps to be taken to address this in the action plan below.			
Comments:				
Action Plan:				
2	Has the ISSPM been appointed in writing by the agency's Senior Information Resource Management Officer (SIRMO)?			
Comments:				
Action Plan:				
3	Has the agency's SIRMO documented the duties of the ISSPM and has the ISSPM acknowledged these duties?			

Comments:
Action Plan:

A management control process is important for ensuring that once a good security profile has been established, it is maintained. The following questions will assist you in addressing this requirement.		YES	NO	PARTIAL
1	Does the agency have a formal management control process? If no, provide an action plan in the space below.			
Comments:				
Action Plan:				
2	Are sufficient management control processes in place to assure that appropriate administrative, physical, and technical safeguards are incorporated into new applications, and into significant modifications to existing applications.			
Comments:				
Action Plan:				
3	Does the management control process document the requirements for each major information system and allow for periodic review of those requirements over the system's life?			
Comments:				
Action Plan:				
4	Does the management control process for applications include security specifications, design reviews, and system tests?			
Comments:				
Action Plan:				
5	Does the management control process include multi-year strategic planning for acquiring and operating information technology?			
Comments:				

Action Plan:				
6	Does the management control process ensure that the ISSPM thoroughly reviews all vendor recommendations and requirements for the configuration of security controls and formally documents compliance or non-compliance of such requirements?			
Comments:				
Action Plan:				
7	Are annual internal control reports provided to the President and Congress?			
Comments:				
Action Plan:				
8	Is there a program to conduct periodic risk analyses on AIS to determine whether security baselines are met and to ensure that appropriate, cost-effective safeguards are incorporated on all new and existing AIS, networks, and facilities?			
Comments:				
Action Plan:				

Contingency planning is an integral part of the USDA information security program. It enables the agency to respond to and recover from unexpected and sudden disruptions of service, preventing minor problems from becoming major and major problems becoming catastrophic. Although a contingency plan will not prevent a natural disaster such as a flood, tornado, and the like, it will mitigate the effects of such unfortunate occurrences. The following questions will assist you in addressing the requirements for contingency planning.		YES	NO	PARTIAL
1	Are there appropriate continuity plans for the agency to ensure continuity of operations? If no, provide an action plan in the space below.			
Comments:				
Action Plan:				
2	Are the plans tested periodically for their adequacy and effectiveness in accordance with business needs?			
Comments:				
Action Plan:				

Many USDA functions rely on vital records and various documents, papers, or forms. These records could be important because of a legal need or because they are the only record of the information. Records can be maintained on paper, microfiche, microfilm, magnetic media, or optical disk. Departmental Regulation 3090-001 provides responsibilities and procedures for identifying and maintaining USDA vital records. Of primary interest from an Information Security perspective is considering the protection of Vital Records for the continuity of USDA operations. The answers to the following questions will assist you in addressing the requirements for protecting vital records.		YES	NO	PARTIAL
1	Are vital records identified in accordance with DR 3090-001? If no, provide an action plan in the space below.			
Comments:				
Action Plan:				
2	Are vital records stored in appropriate locations?			
Comments:				

Action Plan:				
3	Is there a process for assuring that vital records are properly assembled, packed, and arranged for shipment to appropriate storage locations?			
Comments:				
Action Plan:				
4	Are emergency operating records at storage locations periodically inspected? Are they certified for the currency and adequacy of the inventory following each inspection?			
Comments:				
Action Plan:				

The Computer Security Act of 1987 requires training for all employees responsible for the management and use of Federal computer systems that process sensitive information. The USDA DR 3140-001 requires annual information systems security awareness training and that employees and contractors at all levels of USDA are provided with sufficient guidance to discharge their responsibilities relating to AIS security. The answers to the following questions will assist you in addressing the requirements for Security Awareness Training.		YES	NO	PARTIAL
1	Is there a security awareness and training program for the agency? If no, provide an action plan in the space below.			
Comments:				
Action Plan:				
2	Have training and awareness plans been developed for the agency and are they updated annually?			
Comments:				

Action Plan:				
3	Do training plans include (a) training content or subject matter; (b) target audience, including agency and contractor personnel for each of the training content areas; and (c) level of training to be provided for each specific subject matter area and target audience category?			
Comments:				
Action Plan:				
4	Do all personnel who use, operate, or maintain AIS receive training in security awareness and accepted security practices as soon as possible and within a minimum of 60 days of being granted access?			
Comments:				
Action Plan:				
5	Do all personnel who use, operate, or maintain AIS receive an annual threat briefing?			
Comments:				
Action Plan:				
6	Do all personnel who use, operate, or maintain AIS receive annual refresher training?			
Comments:				
Action Plan:				

The USDA is required to comply with the Privacy Act of 1974. This requirement is met with a variety of administrative, management, and technical procedures, policies, and practices. Each agency must ensure that the Information Security Program contributes to the satisfaction of this requirement by answering the following questions. For all "no" responses, provide a response as part of the action plan.	YES	NO	PARTIAL

1	Are there policies and practices regarding the storage, retrievability, access controls, retention, and disposal of Privacy Act Information? If no, provide an action plan in the space below.			
Comments:				
Action Plan:				
2	Have rules, which shall establish procedures for the disclosure to an individual upon his request of his record, been promulgated?			
Comments:				
Action Plan:				
3	Do rules include provisions for providing individuals with access to, and the ability to amend errors in, systems of records consistent with the Privacy Act, Section 552a.d?			
Comments:				
Action Plan:				

The identification and reporting of Information Security violations is part of a sound Information Security Program. Answer the following questions to determine whether the agency contributes to the satisfaction of this requirement.		YES	NO	PARTIAL
1	Are there procedures for forwarding any security violation possibly involving an infraction of Federal criminal laws to the ISSPM and concurrently to the Inspector General?			
Comments:				
Action Plan:				
2	Are there procedures for notifying an individual, who is determined to have been responsible for the unauthorized release or disclosure of classified information, that the action is in violation of applicable USDA regulation DM 3440-1.4?			

Comments:				
Action Plan:				
3	Are copies of all documentation relating to security violations filed in the security violation indexes of the USDA Office of Inspector General, or the agency's ISSPM, and also in the individual's personnel security file?			
Comments:				
Action Plan:				

USDA Regulations 3140-001and 3140-002 establish requirements and provide guidance for ensuring the protection of USDA information resources from viruses. The following questions will help determine the agency compliance with this guidance.		YES	NO	PARTIAL
1	Does the agency have a program designed to minimize the risk of introducing viruses and other malicious software into USDA AIS and networks?			
Comments:				
Action Plan:				
2	Are there procedures for reporting a virus or other malicious software to agency supervisory personnel and the ISSPM? Do procedures call for making the report prior to being fixed?			
Comments:				
Action Plan:				

The requirements for effective computer security for the management and control of federal financial systems are specified in OMB A-123 and OMB A-130 respectively. The following questions will assist in determining your agency's compliance with these requirements.		YES	NO	PARTIAL
1	Does the agency have a five-year plan for a single integrated, efficient financial			

	management system?			
Comments:				
Action Plan:				
2	Does the agency have a policy and a procedure for gathering, processing, recording, and reporting financial management information in the same manner throughout the agency, using uniform definitions?			
Comments:				
Action Plan:				

OMB A-130 and USDA Departmental Regulations specify numerous requirements for personnel security. The following questions will assist in determining the USDA compliance with those requirements at the agency level.		YES	NO	PARTIAL
1	Have personnel security policies and procedures been established and managed to ensure an adequate level of security?			
Comments:				
Action Plan:				
2	Is position sensitivity coded on Optional Form 8, Position Description (or an equivalent agency form) as appropriate?			
Comments:				
Action Plan:				
3	Do individuals assigned to sensitive positions possess the requisite security clearance or background investigation?			
Comments:				
Action Plan:				

4	Do personnel applying for sensitive positions undergo pre-placement background investigations, if required?			
Comments:				
Action Plan:				
5	Are periodic reinvestigations conducted five years after placement, and at least once each succeeding five years, when required?			
Comments:				
Action Plan:				
6	Are contractors subject to the same personnel security requirements as government employees?			
Comments:				
Action Plan:				
7	Are personnel having Military Ready Reserve assignments excluded from assignment to emergency management teams?			
Comments:				
Action Plan:				
8	Are appropriate supervisors, security professionals, and on-site personnel who operate ADP equipment approved for access to all types of restricted access data contained in the system and instructed on appropriate security procedures before being granted unescorted system access?			
Comments:				
Action Plan:				

Following are the communications requirements, which are assessed at the Agency level, to determine compliance with Federal and USDA guidelines. Respond to each question and provide input for the action plan for a response of no.		YES	NO	PARTIAL
1	Does the ISSPM maintain a list of approved Electronic Funds Transfer (EFT) authentication equipment and software techniques?			
Comments:				
Action Plan:				
2	Is off-the-shelf encryption equipment for communications security compliant with Federal Standard 1027 or is it endorsed equipment from the commercial COMSEC Endorsement Program?			
Comments:				
Action Plan:				
3	Is there a written key management plan for the handling and safeguarding of keying material?			
Comments:				
Action Plan:				
4	Is all key material used for the protection of classified national security or sensitive information generated, distributed, stored, and destroyed in a secure and controlled manner?			
Comments:				
Action Plan:				
5	Are there formal memorandums of understanding (MOU) in place with external agencies that have telecommunication interconnections with the agency?			
Comments:				
Action Plan:				

Following are the computer requirements, which are assessed at the Agency level, to determine compliance with Federal and USDA guidelines. Respond to each question and provide input for the action plan for a response of no.		YES	NO	PARTIAL
1	Are there procedures to govern the use of personally owned computers or software to process, access, or store sensitive information?			
Comments:				
Action Plan:				
2	Are there procedures to ensure that sensitive data that has been written to the hard drive of a personally owned computer is completely erased when it is no longer needed, to preclude disclosure or data corruption?			
Comments:				
Action Plan:				
3	Are PC hard disk drives, network file servers, and other media used to handle agency information formatted between the time they are received and put into use?			
Comments:				
Action Plan:				
4	Are procedures in place to ensure the secure destruction of discarded computer material, to preclude unauthorized disclosure?			
Comments:				
Action Plan:				
5	Are procedures in place to ensure that computers are only started up (boot-up) from the original write-protected system master or a trusted copy?			
Comments:				

Action Plan:				
6	Are there procedures for ensuring that portable computer systems such as laptops, that leave agency-controlled areas, are scanned for viruses before and after connecting to Agency systems or software?			
Comments:				
Action Plan:				
7	Are there procedures governing the downloading of software obtained electronically from bulletin boards?			
Comments:				
Action Plan:				
8	Is there written guidance concerning the labeling of magnetic media?			
Comments:				
Action Plan:				

ADP Facility Assessment Guide

This assessment should be completed by the ADP Facility ISSPM or designated alternate. Answer all questions. Provide supplemental information as appropriate. All "No" answers must include an action plan that describes how the requirement will be met, as well as a schedule for completion of the plan.

Facility Identification:

Facility		
Address		
Responsible Manager		Phone:
ADP Facility ISSPM		Phone:
Describe ADP facilities at this location		
Identify ADP equipment at this location.		
Date of last Assessment		

The USDA DR 3140-001 requires that USDA entities develop and implement a comprehensive risk management program, which ensures that security risks are identified and evaluated and appropriate countermeasures are implemented. This includes the development of information system security plans, contingency plans, certification and accreditation of sensitive systems, and physical security, to include access control. The following questions will assist you in addressing this requirement.		YES	NO	PARTIAL
1	Is responsibility for the security of the installation assigned to a management official knowledgeable in information technology and security matters?			
Comments:				
Action Plan:				
2	Does the departmental ISSPM or ADP Facility ISSPM review and approve requirements and specifications for the acquisition or operation of information technology installations, equipment, software, and related services?			
Comments:				
Action Plan:				
3	Is there a Management Control Plan, which identifies component inventory risk ratings (high, medium, low), material weaknesses, and other areas of management concern?			
Comments:				
Action Plan:				
4	Has the Management Control Plan been updated in the last year?			
Comments:				
Action Plan:				
5	Is there a current Risk assessments that identifies the types of threat and the appropriate physical protection measures to the facility?			
Comments:				

Action Plan:				
6	Are appropriate technical, administrative, physical, and personnel security controls in place at the facility?			
Comments:				
Action Plan:				
7	If not, has the Senior Information Resource Management Officer (SIRMO) submitted a written exception for all facilities that cannot meet the baseline physical security requirements?			
Comments:				
Action Plan:				
8	Is there a disaster recovery and continuity of operation plan for the facility?			
Comments:				
Action Plan:				
9	Is the disaster recovery and continuity of operation plan tested periodically to ensure it can be implemented if needed?			
Comments:				
Action Plan:				

The USDA DR 3140-001 requires that, as part of a comprehensive risk management program, USDA entities develop and implement physical security, to include access control. The following questions will assist you in addressing this requirement.		YES	NO	PARTIAL
1	Is access to computer rooms and telecommunications facilities controlled?			
Comments:				
Action Plan:				
2	Does the facility ISSPM maintain a current access roster that identifies each individual requiring routine unescorted access?			
Comments:				
Action Plan:				
3	Are escorts provided for unauthorized individuals at all times?			
Comments:				
Action Plan:				
4	Do escorts have authorization for access to all areas of the facility?			
Comments:				
Action Plan:				
5	Do escorts have any training to ensure they are aware of their responsibilities?			
Comments:				
Action Plan:				
6	Does the facility ISSPM maintain a record of escorted visitors? How long is it kept?			

Comments:				
Action Plan:				
7	Are contractors and vendors subject to the same security controls as government employees?			
Comments:				
Action Plan:				
8	Are maintenance personnel logged-in and escorted when visiting communications facilities?			
Comments:				
Action Plan:				
9	Are facilities locked at all times when authorized personnel are not present?			
Comments:				
Action Plan:				
10	Are precautions in place to prevent unauthorized access to computers and terminals, when not in use?			
Comments:				
Action Plan:				
11	Is there a process to ensure that electronic media does not contain sensitive data before it leaves facility control?			
Comments:				

Action Plan:				
12	Are file servers located in a restricted area?			
Comments:				
Action Plan:				
13	Are controls in place to ensure that file servers are accessed only by authorized personnel?			
Comments:				
Action Plan:				
14	Are personnel who are responsible for the operation and maintenance of system hardware and software approved for access to all types of restricted-access data contained in the system and instructed on appropriate security procedures before being granted unescorted access?			
Comments:				
Action Plan:				
15	Is there a policy in place, and is it included in security awareness training, that terminals, workstations and networked personal computers should never be left unattended when a user ID and password have been logged in?			
Comments:				
Action Plan:				
16	Is there a Trusted Facility Manual or other documentation that provides guidance to the ADP security administrator with respect to running a secure facility?			
Comments:				

Action Plan:

The USDA DR 3140-001 requires that, as part of a comprehensive risk management program, USDA entities develop and implement physical security for the protection of computer equipment. The following questions will assist you in addressing this requirement.		YES	NO	PARTIAL
1	Is physical security for the central computer facilities commensurate with, or exceeding, the minimum requirements of the most restrictive category (or highest classification) of information that may be processed by the system?			
Comments:				
Action Plan:				
2	Are perimeter walls slab to slab in construction and permanently attached to true floor and true ceiling?			
Comments:				
Action Plan:				
3	Do ground level and second story windows have positive locking devices installed?			
Comments:				
Action Plan:				
4	Are doors to an AIS or telecommunications facility solid wood or metal at least 1-3/4 inches thick?			
Comments:				
Action Plan:				
5	Are doors secured with deadbolt locks with a one-inch throw.			
Comments:				

Action Plan:				
6	Is the distribution of keys controlled?			
Comments:				
Action Plan:				
7	Are keys “off-master” in buildings shared with other entities?			
Comments:				
Action Plan:				
8	Are cipher locks used to control access to computer facilities?			
Comments:				
Action Plan:				
9	Are cipher combinations at least four numbers?			
Comments:				
Action Plan:				
10	Are cipher combinations changed at least every six months or when anyone with the combination no longer requires access?			
Comments:				
Action Plan:				
11	Are cipher locks used to control access after duty hours?			
Comments:				

Action Plan:				
12	Is the cipher lock combination protected by shielding or is there a policy that personnel protect the combination when they are accessing the facility?			
Comments:				
Action Plan:				
13	Are precautions in place to inhibit theft of government property?			
Comments:				
Action Plan:				

The digital PBX is a key component of the USDA telecommunications infrastructure and must be protected to ensure effective and efficient delivery of service and to ensure its role in the continued operation of the USDA. The following questions will assist in determining whether adequate protections are provided for the digital PBX at each facility.		YES	NO	PARTIAL
1	Does you facility house a digital PBX? If the answer is yes, answer the remaining questions.			
Comments:				
Action Plan:				
2	Do digital switch and key system facilities have adequate physical and procedural controls?			
Comments:				
Action Plan:				
3	Are PBX systems, voice mail systems, and their administrative terminals with other equipment requiring human access co-located?			
Comments:				

Action Plan:				
4	Is this equipment password protected?			
Comments:				
Action Plan:				
5	Is the password changed at least semi-annually?			
Comments:				
Action Plan:				
6	Does the facility ISSPM maintain a copy of the vendor’s policy regarding password administration in instances where the vendor controls the remote maintenance password for the systems maintenance and remote maintenance access?			
Comments:				
Action Plan:				

AIS Assessment Guide

This assessment should be completed by the AIS ISSPM, system owner, or designated alternate. Answer all questions. Provide supplemental information as appropriate. All "No" answers must include an action plan that describes how the requirement will be met, as well as a schedule for completion of the plan. Typically the information in the action plan would result in an update of the AIS Security Plan.

In addition to completing this assessment guide, the AIS ISSPM, system owner, or designated alternate must also complete the appropriate AIS Platform checklist included at the end of this assessment guide. Checklists have been included for Novell, Windows NT, HP and SCO UNIX, and AS400.

AIS Identification:

AIS:	
Location:	
Responsible Manager:	Phone:
Responsible ISSPM	Phone:
Date of last Assessment:	

System/application description:

Is this AIS a: mainframe _____
client server _____
stand-alone PC _____
web-based _____

What Operating System (OS) does this AIS use: ________________

What database does this AIS use: ____________

What types of data does this AIS store, process or transmit (check all that apply):
Privacy Act: _____
Financial: _____
Procurement: _____
Other: _____

What is the need for availability, integrity and confidentiality of this data (High, Medium, Low):

	Availability	Integrity	Confidentiality
Privacy Act			
Financial			
Procurement			
Other			

The USDA DR 3140-001 requires that USDA entities develop and implement a comprehensive risk management program which ensures that security risks are identified and evaluated, and appropriate countermeasures are implemented. This includes the development of information system security plans, contingency plans, certification and accreditation of sensitive systems, and physical security to include access control. The following questions will assist you in addressing this requirement.		YES	NO	PARTIAL
1	Does the AIS or network store, process or transmit sensitive data?			
2	Does the AIS or network have a current risk analysis or a threat assessment that was conducted within the last three years?			
Comments:				
Action Plan:				
3	Are copies of risk assessments kept in a secure area commensurate with the sensitivity of information contained in the report?			
Comments:				
Action Plan:				
4	Have any requests for exceptions to USDA security requirements been submitted? If so, describe them below.			
Comments:				
Action Plan:				
5	Is the AIS or network formally accredited?			
Comments:				

Action Plan:				
6	Has a Certifying Official (Departmental ISSPM) formally certified, in writing, that the system meets all applicable Federal policies, regulations, and standards, based on the results of tests demonstrating that the installed security safeguards are adequate for the application?			
Comments:				
Action Plan:				
7	Was security testing conducted in support of the Certification and Accreditation process?			
Comments:				
Action Plan:				
8	If not accredited, does the AIS or network have an interim approval to operate?			
	Comments:			
	Action Plan:			

The Computer Security Act of 1987 and OMB Circular No. A-130, Appendix III require all Federal agencies to plan for the security of all sensitive information systems throughout their life cycle. USDA agencies are further required to ensure that security is included in all stages of a system’s life cycle as defined in DM 3140-1. The following questions will assist you in addressing this requirement.		YES	NO	PARTIAL
1	Does the AIS or network comply with the Federal Information Processing Standards (FIPS)? For example FIPS 140 establishes the encryption standard?			
Comments:				
Action Plan:				
2	Did the AIS or network incorporate appropriate technical, administrative, physical and personnel security features during the conceptual design phase?			
Comments:				
Action Plan:				
3	Did the designated system owner or responsible ISSPM define and approve security requirements and specifications prior to acquiring or starting formal development of an AIS application?			
Comments:				
Action Plan:				
4	Were design reviews and system tests conducted and approved prior to placing the application or network into operation?			
Comments:				
Action Plan:				
5	Are results of design reviews and system tests fully documented and maintained in the official agency records?			
Comments:				

Action Plan:				
6	Is there a configuration management plan for this AIS or network and has it been implemented?			
Comments:				
Action Plan:				
7	Is every change made to documentation, hardware, and software/firmware reviewed and approved by the ISSPM, Network Security Officer, or the available security staff?			
Comments:				
Action Plan:				
8	Is every change made to documentation, hardware, and software/firmware documented?			
Comments:				
Action Plan:				
9	Can the completed change be verified to be functionally correct, and for trusted systems and networks, consistent with the security policy of the system or network through the process of a configuration audit?			
Comments:				
Action Plan:				
10	Is there a process in place to ensure that each site receives the appropriate version of the system or network in the case of a change that will be used at multiple sites?			
Comments:				

Action Plan:				
11	Is there a process in place to ensure that financial management information (from financial management systems) is recorded and reported in the same manner throughout the agency, using uniform definitions?			
Comments:				
Action Plan:				

Contingency planning is an integral part of the USDA information security program. It enables the agency to respond to and recover from unexpected and sudden disruptions of service, preventing minor problems from becoming become major and major problems may becoming catastrophic. Each AIS must have its own plan and take precautions such as backing up data to ensure it can recover when necessary. Although a contingency plan will not prevent a natural disaster such as a flood, tornado, and the like, it will mitigate the effects of such unfortunate occurrences. The following questions will assist you in addressing the requirements for contingency planning.		YES	NO	PARTIAL
1	Does the AIS or network have disaster recovery and contingency plan?			
Comments:				
Action Plan:				
2	Are the plans tested periodically for their adequacy and effectiveness?			
Comments:				
Action Plan:				
3	Is new software backed up immediately, retaining the original distribution diskettes in a safe and secure location?			
Comments:				
Action Plan:				
4	Are data files backed up frequently?			
Comments:				
Action Plan:				
5	Are data files stored off-site or in a secured environment?			
Comments:				
Action Plan:				

6	Are damaged software programs restored from the original diskettes, not from regular backups?			
Comments:				
Action Plan:				
7	Is hardware and software scanned before it is used to verify that it does not contain any viruses?			
Comments:				
Action Plan:				

Ensuring that the AIS has appropriate access controls which limit access to the AIS to only those individuals who should have access is a key requirement of ensuring that the appropriate safeguards are in place for the AIS. The following questions will assist you in determining that this requirement has been met.		YES	NO	PARTIAL
1	Does the system assure that users without authorization are not allowed access to the data?			
Comments:				
Action Plan:				
2	Does the system define and control access between named users and system resources (e.g., files and programs)?			
Comments:				
Action Plan:				
3	Do system owners have the capability to specify, at their discretion, who (by individual users or user, groups, etc.) may have access to their data?			
Comments:				
Action Plan:				
4	Does the system protect authentication data so that it may not be accessed by an unauthorized user?			
Comments:				
Action Plan:				
5	Are passwords shared by multiple users?			
Comments:				
Action Plan:				

6	Does the system prevent a user from choosing a password that is already associated with another user ID?			
Comments:				
Action Plan:				
7	Are passwords stored in a one-way encrypted form?			
Comments:				
Action Plan:				
8	Does the system automatically suppress or fully blot out the clear-text representation of the password on the data entry device?			
Comments:				
Action Plan:				
9	Does the system block any demonstration of password length (i.e., the cursor should not move upon input)?			
Comments:				
Action Plan:				
10	Does the system allow null passwords during normal operation?			
Comments:				
Action Plan:				
11	Are passwords and user IDs immediately removed when an authorized user no longer needs access to the system?			
Comments:				

Action Plan:				
12	Does the system allow users to change their passwords ?			
Comments:				
Action Plan:				
13	Does the system force users to change their passwords at least every 60 days, and at least every 30 days for user IDs that may acquire privileges?			
Comments:				
Action Plan:				
14	Does the system notify the user to change their password before the password expiration date?			
Comments:				
Action Plan:				
15	Are users prevented from using the same password within six months of changing them?			
Comments:				
Action Plan:				
16	Does the system provide a method of ensuring the complexity of user-entered passwords (e.g., eight characters minimum length)?			
Comments:				
Action Plan:				
17	Are vendor-supplied passwords, including those for software packages and maintenance accounts, changed as soon as the system has been installed?			

Comments:				
Action Plan:				
18	Are storage objects (e.g., core area, disk file, etc.) cleared before being assigned, allocated, or reallocated to a system user?			
Comments:				
Action Plan:				

The USDA DR 3140-001 requires that USDA entities administer a personnel security program that identifies, categorizes, and defines personnel security requirements and controls to ensure that personnel are granted access only on a need-to-know basis. The Computer Security Act of 1987 requires training for all employees responsible for the management and use of Federal computer systems that process sensitive information. The USDA DR 3140-001 further requires annual information systems security awareness training and that employees and contractors at all levels of USDA are provided with sufficient guidance to discharge their responsibilities relating to AIS security. Some of those requirements are met at the agency or facility and have been addressed in the corresponding assessment guide. The answers to the following questions will assist you in meeting the requirements for Personnel Security and Security Awareness Training at the AIS level.		YES	NO	PARTIAL
1	Are personnel granted access on a need-to-know basis, and when that need no longer exists, is their access canceled?			
Comments:				
Action Plan:				
2	Are personnel trained on the security features of the AIS and how to use them within 60 days of being granted access?			
Comments:				
Action Plan:				
3	Is continuing training provided whenever there is significant change in the telecommunications and AIS environment or procedures?			

Comments:				
Action Plan:				
4	Do personnel who install, operate, maintain, or use the AIS or network acknowledge their security responsibilities and attest their understanding of security practices in writing?			
	Comments:			
	Action Plan:			

The USDA DR 3140-001 requires that USDA systems will employ robust authentication measures for dial-in and Internet access. Activity logging and use of encryption also provide a means to ensure anyone does not gain unauthorized access to sensitive data while it is being transmitted. The following questions will help you determine whether communications precautions meet USDA standards.		YES	NO	PARTIAL
1	Does the AIS or network have dial-up access? If yes, answer the following questions.			
Comments:				
Action Plan:				
2	Is dial-up access protected with Federal government approved devices or techniques that provide explicit user identification and authentication, and audit trails?			
Comments:				
Action Plan:				
3	Is there a well-administered user name and authentication process for controlling each user having dial-in access?			
Comments:				

Action Plan:				
4	If used, are "Barrier Codes" set to the maximum length allowed by the PBX system?			
Comments:				
Action Plan:				
5	Is a dial-back authentication system used as an alternative for user identification, authentication, and audit trails?			
Comments:				
Action Plan:				
6	Is the system's own journaling or logging capability used to monitor all communications activity with the host, to determine system or network usage, identify user difficulties, and uncover intrusion attempts?			
Comments:				
Action Plan:				
7	Is sensitive information encrypted using NSA Type 2 encryption, NSA endorsed Data Encryption Standard (DES), or DES devices determined to be compliant with the appropriate FIPS standards?			
Comments:				
Action Plan:				

Control of media is an important aspect of an effective Information Security Program. The following questions will assist you in determining that this aspect is being addressed by your AIS.		YES	NO	PARTIAL
1	Does the AIS produce media such as magnetic tape or removable diskettes? If the answer is yes, answer the following questions.			

Comments:				
Action Plan:				
2	Is media labeled to reflect the sensitivity of the data that it contains?			
Comments:				
Action Plan:				
3	Are procedures in place to ensure the secure destruction of discarded computer material, to preclude unauthorized disclosure?			
Comments:				
Action Plan:				
4	Is media purged before submitting it for destruction?			
Comments:				
Action Plan:				
5	Is degaussing conducted with an approved degausser?			
Comments:				
Action Plan:				
6	Is overwrite software protected at the level of the media it purges?			
Comments:				
Action Plan:				
7	Is only new media used for making copies for distribution?			

Comments:
Action Plan:

The USDA DR 3140-001 requires that USDA systems ensure individual accountability for data, information, and all IT resources to which individuals have access. The primary way to ensure accountability is through system audit features. The answers to the following questions will assist you in determining whether system audit features provide sufficient accountability.		YES	NO	PARTIAL
1	Can the system create and maintain and audit trail, and protect it from modification, unauthorized access, or destruction?			
Comments:				
Action Plan:				
2	Can the system record log on/log off, change of password, creation, deletion, opening, and closing of files, program initiation, and all actions by system operators, administrators, and security officers? If no, provide an action plan in the space below and skip the remaining questions.			
Comments:				
Action Plan:				
3	For each recorded event, can the audit record identify: date and time of the event, user, type of event, and the success or failure of the event?			
Comments:				
Action Plan:				
4	Is the audit data protected by the system so that read access to it is limited to those who are authorized for audit data?			
Comments:				

Action Plan:				
5	For log on, log off, and password change, is the origin of the request (e.g., terminal ID) included in the audit record?			
Comments:				
Action Plan:				
6	For file-related events, does the audit record include the file's name?			
Comments:				
Action Plan:				
7	Can the Departmental ISSPMs selectively audit the actions of one or more users based on individual identity?			
Comments:				
Action Plan:				

In accordance with OMB Circular No. A-130, Appendix III, each general support system and major application will have developed a security plan consistent with guidance issued by NIST, SP 800-18, as a minimum.		YES	NO	PARTIAL
1	Does the AIS or network have a security plan?			
Comments:				
Action Plan:				
2	Is the security plan reviewed and updated annually?			
Comments:				

Action Plan:				
3	Does the AIS have a Security Features User's Guide that describes the system's security features and how to use them? This may be a separate document or a chapter in other documentation, such as a user manual.			
Comments:				
Action Plan:				
4	Does the AIS have a Trusted Facility Manual that presents cautions about functions and privileges that should be controlled and provides guidance on how to maintain a secure system? This may be a separate document or a chapter in other documentation, such as an administrator's manual.			
Comments:				
Action Plan:				
5	Is there a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing?			
Comments:				
Action Plan:				
6	Is the AIS or network design documented?			
Comments:				
Action Plan:				